REMARKS

The following remarks are responsive to the Office Action of December 9, 2008, which was made Final.

At the time of the Office Action, claims 1-30 were pending. Claim 13 was rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. (U.S. Patent No. 5,987,138). Claims 1-2, 11 and 16-17 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al. (U.S. Patent No. 5,946,397). Claims 12 and 18 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al., and further in view of Brickell (U.S. Patent No. 7,165,181). Claims 19 and 27 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al., and further in view of Kasahara et al. (U.S. Patent No. 6,788,788). Claims 3 and 4 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al., and further in view of Arditti et al. (U.S. Patent No. 6,125,445). Claims 5-10 and 23-26 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al. and Arditti et al., and further in view of Kasahara et al. Claims 20-22 and 28-30 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi et al. and Kasahara et al., and further in view of Arditti. Claim 14 was rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al., and further in view of Kasahara et al. Claim 15 was rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of Kasahara et al., and further in view of Arditti et al. Claim 8 was rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Claim 13 was also objected to.

Applicants respectfully submit that the above amendments to the claims overcome the formal objection and rejection, and that the amended claims are allowable at least for the reasons set forth below.

The Formal Objection and Rejection

In response to the rejection of claim 8 under 35 U.S.C. §112, second paragraph, as being indefinite, claim 8 is being amended to remove the word "substantially" to which the

Examiner objects. In response to the objection to claim 13, claim 13 is being amended to change the term "power device" to "prover device." Accordingly, Applicants respectfully request the Examiner to withdraw this rejection and objection.

The 35 U.S.C. §103(a) Rejection of Claim 13

Claim 13 was rejected under 35 U.S.C. §103(a) as obvious over Gilbert. Applicants respectfully submit that amended claim 13 is allowable for at least the following reasons.

In the rejection, the Examiner has acknowledged that Gilbert does not disclose raising the generic number (g) to a second power, modulo the modulus, having a third exponent (er) equal to the first exponent (e) of the public key multiplied by a random integer (r) kept secret by the first entity. However, the Examiner contends that it would have been obvious to multiply the exponent with another number in order to achieve a desired security level, and that using a resulting product as an exponent would be equivalent to using two numbers multiplied together.

Applicants respectfully submit that amended claim 13 does not recite the mere multiplication of two numbers. Rather, claim 13 relates explicitly to the multiplication of the first element of a public key "e" with a random number "r." Applicants respectfully submit that Gilbert fails to teach or suggest using an element of proof with an exponent resulting from the product of two numbers. Rather, Gilbert discloses an identification protocol using the calculation of an element of proof where "e" is a public exponent.

Applicants respectfully submit that the passage in column 8, lines 33-44 of Gilbert that was cited by the Examiner only refers to the fact that the public exponent "e" is a small integer equal to or greater than 3 but below 100. Although such a small integer, when not a prime number, could be obtained by a multiplication of two other integers, this passage does not teach or suggest performing such a multiplication, since Gilbert merely discloses that a public exponent "e" should be used in the identification process of claimant P. Furthermore, Applicants submit that the complete exponent "e" of the element of proof "x" in Gilbert is therefore necessary known by both the claimant P

and the verifier V, in order for the verifier V to identify the claimant P. There is no reason in Gilbert to multiply two integers in the claimant P, in order to obtain a public exponent shared by the two entities.

Applicants further respectfully note that column 8, lines 33-45 of Gilbert clearly state that the choice of having a small public exponent "e" (below 100) offers advantages, like reducing the number of secrets or passes for an equal security level. This passage of Gilbert therefore teaches keeping the public exponent "e" as small as possible. Accordingly, Gilbert teaches away from multiplying the public exponent by another integer, like in the claimed embodiments of the present invention, since such a multiplication would increase the value of such an exponent. Also, all the examples of exponent "e" given in Gilbert ("5" or "17" in column 8, lines 43- 44; "5" in column 9, line 61; "5" in column 10, line 17, and "17" in column 10, line 26) are prime numbers, which further teaches away from using an exponent resulting from the product of two integers.

In addition, Applicants submit that Gilbert fails to hint at using an exponent resulting from the product of a public key integer with a random number. That is, not only does Gilbert fail to teach multiplying two integers to obtain the exponent of the element of proof "x," but Gilbert also fails to teach or suggest using the multiplication of a first integer "e" with a second random number "r."

In the embodiment of the present invention as recited in claim 13, the element of proof "x," generated by the entity (A), has an exponent which is the product of a public key "e" and a random number "r." As such, this exponent as a whole is random and not known by the entity (B). This is intended to increase the security level of the identification process.

As can be appreciated by one skilled in the art, the use of such a random number "r" increases the security level of the identification process, since only the entity (A) that generates this random number "r" can generate the element of proof "x." This advantage is clearly described, for example, on page 17, lines 8 to 12 of the present

application. This passage also shows that, since only the entity (A) is capable of generating "x" from the random number "r," the number "x" is a first element of proof, identifying the entity (A). Since identification of the entity A by the entity B requires the k times iteration of the protocol shown in Fig. 1 (See, e.g., the description, page 16, lines 17-22 of the present application), by using such a random number "r," the entity (A) will be able to generate different elements of proof "x" for each iteration of the process shown in Fig. 1. Each of these elements of proof can only be generated by the entity (A).

On the contrary, the element of proof "x" in Gilbert has an exponent "e" known by both the claimant P and the verifier V. This is necessary for the verifier to be able to calculate $H(m,y^e)$, as mentioned in column 9, lines 10-15 of Gilbert. For the method of Gilbert to be able to work, the exponent of the element of proof "x" generated by the claimant P must be known by the verifier V. Such an exponent cannot therefore be random in Gilbert, and Gilbert therefore teaches away from using a random number as an exponent for the element of proof generated by the claimant P. As a consequence, Gilbert teaches away from using an element of proof with an exponent resulting from the product of a public key integer with a random number.

Furthermore, Applicants respectfully submit that Gilbert teaches decreasing the public exponent "e," whereas the claimed embodiment of the present invention aims at increasing the public exponent. As discussed above, Gilbert aims at decreasing the public exponent "e," since Gilbert aims at reducing the number of secrets or passes compared to other schemes (see column 8, lines 33-44). On the contrary, the embodiment of the present invention as recited in claim 13 aims at increasing the exponent of the first element of proof "x," since the claimed embodiment generates a first element of proof "x" with a first calculation consuming considerable resources, which can be carried out before the transaction as described, for example, on page 9, lines 14-24 of the present application. Applicants respectfully submit that Gilbert and the claimed embodiment of the present invention therefore have opposite purposes with respect to the value of the exponent "e," and as such, Gilbert does not teach or suggest using a product of integers since this would increase, rather than decrease, the public exponent "e."

Applicants also respectfully submit that the use of a first element of proof "x" with an exponent being the product of a public exponent "e" and a random number "r" renders the identification process of the claimed embodiment of the present invention much safer than the process in Gilbert. Applicants submit that as can be appreciated by one skilled in the art, the number $x=r^{e,}$ as calculated in Gilbert, can be deciphered in a reasonable amount of time, since "e" is a small integer. With the knowledge of "e," which is a public exponent, a third party intercepting the element of proof "x" can quite easily derive "r" (because "e" is a small integer, this backward calculation is easier), and can try then to authenticate with the verifier in place of the claimant P.

However, with the number $x=g^{er}$ as calculated in the claimed embodiments of the present invention, the same third party, knowing the public exponent "e" and intercepting the value "x," is unable to derive "g," because of the product with the random number "r." The third party is therefore unable to authenticate with the verifier in place of the entity (A). Again, Applicants submit that this is a clear advantage of the embodiments of the present invention over Gilbert that neither Gilbert, nor any other cited references, teaches or suggests.

Applicants thus submit that for at least these reasons, one skilled in the art would not have found the embodiment recited even in amended independent claim 13 obvious in view of Gilbert.

The Other 35 U.S.C. §103(a) Rejections

Claims 1-2, 11 and 16-17 were rejected under 35 U.S.C. §103(a) as obvious over Gilbert et al. in view of M'Raihi. In this rejection, the Examiner admits that Gilbert fails to teach the "verifying" feature as recited in independent claims 1 and 16. Nevertheless, for this feature, the Examiner relies on the teachings of M'Raihi and concludes that one skilled in the art would have found it obvious to have modified the Gilbert system and method in accordance with the teachings of M'Raihi to have achieved the embodiments of the present

invention as recited in the rejected claims.

However, Applicants respectfully note that independent claims 1 and 16 are being amended to explicitly recite the feature of multiplying a first exponent by a random integer as discussed above in detail with regard to the rejection of independent claim 13. Other minor amendments have been made in order to distinguish more clearly the exponent of the public key from the exponents of the different powers involved in the claims. For reasons similar to those discussed above, Applicants respectfully submit that Gilbert fails to teach or suggest this feature as now recited in independent claims 1 and 16. In addition, Applicants submit that M'Raihi is being cited as allegedly teaching the claimed "verifying" operation. Applicants submit that M'Raihi does not teach or suggest the feature of multiplying a first exponent by a random integer as recited in the amended claims.

Accordingly, Applicants submit that M'Raihi fails to make up for the deficiencies in the teachings of Gilbert. Hence, one skilled in the art would not have found it obvious or possible to have modified Gilbert in accordance with the teachings of M'Raihi to have achieved the embodiments of the present invention even as recited in independent claims 1 and 16. Thus, all claims should be allowable over these references.

Concerning the rejections of the dependent claims based on Gilbert in various combinations with M'Raihi, Brickell, Kasahara and Arditti, Applicants submit that M'Raihi is being cited for the reasons discussed above, and Brickell, Kasahara and Arditti are being cited as allegedly teaching the specific features of the dependent claims against which they are applied. Applicants submit, however, that these references fail to make up for the deficiencies in the teachings of Gilbert as discussed above. Hence, one skilled in the art would not have found it obvious or possible to have modified Gilbert in accordance with the teachings of these references to have achieved the embodiments of the present invention even as recited in independent claims 1 and 16. Thus, all claims should be allowable.

.

Conclusion

The application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
Joseph J. Buczynski, Reg. No. 35,084
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: February 9, 2009

CH01/ 25298881.1